ABSTRACT

A test method for Internet-Protocol packet networks that verifies the proper functioning of a dynamic pinhole filtering implementation as well as quantifying network vulnerability statistically, as pinholes are opened and closed is described. Specific potential security vulnerabilities that may be addressed through testing include: 1) excessive delay in opening pinholes, resulting in an unintentional denial of service; 2) excessive delay in closing pinholes, creating a closing delay window of vulnerability; 3) measurement of the length of various windows of vulnerability; 4) setting a threshold on a window of vulnerability such that it triggers an alert when a predetermined value is exceeded; 5) determination of incorrectly allocated pinholes, resulting in a denial of service; 6) determining the opening of extraneous pinhole/IP address combinations through a firewall which increase the network vulnerability through unrecognized backdoors; and 7) determining the inability to correlate call state information with dynamically established rules in the firewall.